U.S. CONSUMER PRODUCT SAFETY COMMISSION
4330 EAST WEST HIGHWAY
BETHESDA, MD 20814

STATEMENT OF COMMISSIONER ELLIOT F. KAYE REGARDING A FRAMEWORK OF SAFETY FOR THE INTERNET OF THINGS

January 31, 2019

Sixty billion connected devices and counting, the Internet of Things (IoT) is already providing consumers with conveniences and benefits only imagined a few years ago. But this staggering pace of innovation needs to be tempered with foresight, because product safety cannot be an afterthought with connected devices. Strategies to prevent foreseeable or intentional misuse resulting in product safety hazards must be built into connected systems from the first product concept to the final recycling of the worn out product.

Today, I am releasing a framework that my office and I prepared, which is a compilation of considerations for designing safer connected devices. It provides technology-neutral best practices to incorporate consumer product safety in the design and deployment of devices, software and systems.

This IoT paper is just the beginning of a conversation about injury prevention in this area. I do not expect to have foreseen every potential hazard pattern or to have produced the definitive exegesis on every product safety concern that may arise in IoT; but this is a good place to start the discussion.

A FRAMEWORK OF SAFETY for the Internet of Things:

Considerations for Consumer Product Safety

Abstract

How manufacturers can prevent death, physical injury or illness resulting from mechanical contact, electrical or thermal energy release or toxic exposures associated with connected devices

Elliot F. Kaye and Jonathan D. Midgett, PhD

Elliot F. Kaye is a Commissioner at the U.S. Consumer Product Safety Commission.

Jonathan D. Midgett, PhD is the Senior Science and Policy Advisor in the Office of Commissioner Kaye.

This paper is issued by the Office of Commissioner Kaye. The views expressed in this paper are those of Commissioner Kaye and Dr. Midgett and do not necessarily represent those of the Commission or Commission staff. This framework is not a binding or enforceable rule or Commission guidance and does not change any person's rights, duties or obligations under the Consumer Product Safety Act or any other Act administered by the Commission. Information in this document may be changed or superseded.

A FRAMEWORK OF SAFETY
FOR THE INTERNET OF THINGS

Introduction

The ever-expanding ecology of everyday objects with electronic interconnections is commonly referred to as “the Internet of Things” (IoT).

The purpose of this framework is to provide an overview of technology-neutral best practices to ensure consumer product safety in the design and deployment of devices, software and systems used with Internet-connected consumer products. Product designers need to be aware of the capabilities of every component of their final product and predict unintentional uses and intentional misuses that could lead to foreseeable hazardous conditions. These best practices will help ensure that devices and components of devices are designed to prohibit unsafe system actions, command and control critical safety functions, and signal precursors to hazardous events as reliably as possible over the expected lifespan of the system.

“Consumer product safety” in the context of this framework is defined as *the prevention of death, physical injury or illness resulting from mechanical contact, electrical or thermal energy release or toxic exposures*. Examples of physical injury or illness could include but are not limited to burns, lacerations, strains, contusions, suffocation, strangulation, poisoning, illness, disease, seizures or internal injuries. Physical injury or illness can result from incidents caused by the distraction or isolation of product users from their environment, which leads to or contributes to a chain of events causing injury or illness; or incidents caused by criminal activities that use Internet-connected consumer products to intentionally or unintentionally injure, violate or expose victims to hazardous substances or injurious events.

This framework is <u>not</u> specifically intended to address issues related to the personal *privacy* or data *confidentiality* of information, such as the theft of identity, money or personal information (for cybersecurity best practices, see Appendix A). While the best practices for injury prevention, information security and consumer privacy often overlap—indeed, many of the countermeasures used to prevent identity theft may appear in the discussion below—*consumer product safety issues are unique and need special consideration*. In addition to the categories of safety risks present in non-IoT versions of products, IoT products involve code safety questions – possible code integrity and availability defects, flaws, vulnerabilities, malfunctions or compromises that can lead to physical harms.

This list of considerations and potential concerns is not comprehensive and will undoubtedly evolve. The goal is to promote discussion and debate about consumer product safety during the still relatively early stages of the proliferation of connected devices across society, rather than wait until incidents and injuries force the discussion (see Appendix A for other white papers). This is an active approach to safety, as opposed to being reactive.

The framework outlines various stakeholder roles in the development and deployment of IoT devices as well as procedures to, as much as possible, anticipate and prevent hazardous conditions. Ultimately, every engineer, designer and retailer of IoT devices plays an important part in helping consumers avoid accidental illness, injury or death associated with the use of interconnected objects.

I. Manufacturers' and Retailers' Roles and Responsibilities

- Manufacturers and retailers of IoT devices and software should anticipate safety concerns as new capabilities are added to the IoT ecosystem or products are modified, updated or re-purposed throughout their useful lives until the devices are disposed of for recycling or waste collection.

- Safety guidance activities and procedures should be performed during the concept phase of product development and monitored at every major milestone as the product is manufactured, placed into use, experiences defects, flaws, vulnerabilities, malfunctions and compromises that are reported to the manufacturer, corrected, modified or updated after purchase, and through end-of-life until recycled or discarded.

- Safety requires a coordinated effort among all of the professionals developing a product, including engineers, designers, programmers, marketers and their respective managers.

- Safety requires a corporate receptivity to external reports of defects, flaws, vulnerabilities, malfunctions and compromises and a transparent, easy method for users to submit reports.

- A qualified safety supervisor designated with the authority to provide meaningful influence to the product development processes within a company should be assigned to monitor the development and marketing of each product and product component of an IoT system, including the safety of the software upon which the product relies for functionality. Safety supervisors should be empowered to monitor, reward and encourage a culture of safety and security that extends throughout the entire company. A safety supervisor's authority should be concomitant with the level of risk associated with the product that they are supervising, i.e., potentially fatal products need more extensive safety oversight.

II. Necessary Evaluations for the Development of All IoT Products

Manufacturers should consider the following steps when developing connected devices. While the specific method of risk assessment that should be used is not defined here, many alternatives exist in the field of engineering, as well as best practices in risk modeling of code safety and information security. Existing standards for information security and secure code development should be followed and manufacturers of connected products should pay close attention to the evolution of standards in this industry.

A. Conduct Risk Assessments of Products and Product Systems

Manufacturers should perform an analysis of the likelihood and severity of injury, illness or death for each expected function that a product will perform, every software update and every stage of the lifecycle of the product, including a failure modes and effects analysis (FMEA) that considers user characteristics and reliability, material aging effects, power losses, foreseeable tampering, foreseeable code defects, flaws, vulnerabilities, malfunctions, consumer modification, compromises, sometimes colloquially referred to as “hacking,” and other foreseeable use and misuse events.

Risk assessments should:

- ✓ Include consideration of the intended end user of the system, including use by inexperienced and expert user populations, use by children and the elderly and disabled, and human factors (such as, but not limited to ergonomics, cognition, sensation, perception, and behavioral expectancies). (See Appendix A.)

- ✓ Include an assessment of all components of the product within a system – both mechanical hardware and software components – embedded in an expected environment, including electromagnetic, thermal or kinetic interactions between devices connected to the product and its expected installation environment (garage, kitchen, bedroom, vehicle, school, etc.).

- ✓ Consider any unintended consequences of actuation of any type of energy release (thermal, electrical, kinetic) by users through remote control (users not physically present in the vicinity of the device being activated).

- ✓ Consider unintended interactions of the subject device with other IoT systems in the intended and foreseeable use environments.

- ✓ Consider any unintended consequences of the following types of malfunctions:

    - Manufacturing defects

    - Failure to load a software update

    - Corruption of data during a software update

    - Other data or code corruptions (like sensor aging, damage or power loss; compromise/tampering; consumer modification)

    - Unintended activation

    - Intentional activation during unsafe conditions

- Defaulting to non-personalized settings without warning
- Failure to operate a critical safety function caused by:
  - Loss of connectivity
  - Incompatibility with foreseeable system components
  - Power surge or loss
  - Obsolescence
  - Aging
  - Other degradation (like sensor aging, damage, or power loss; compromise /tampering; consumer modification)
- User error or misuse. (See Appendix A.)

B. Evaluate Component Parts of Products for Safety Criticality

- ✓ Assess how critical each component part including all embedded software, is to the safe operation, safe update and safe use of the product. Potentially critical components include power supplies, sensors, software, software updates, user interfaces, supervisory circuit parts, electronics housings, etc. Components identified as critical for safety must be subjected to controls concomitant with their level of importance to safety.

- ✓ Document safety criticality evaluations at appropriate points throughout the development of a product, so that changes during either design or manufacturing of hardware and software are not overlooked.

III. Potential Countermeasures for Identified Safety Risks

Any safety concerns raised in the risk assessment should be addressed in some manner, preferably using the most effective countermeasures that are feasible, such as:

- ✓ Certification of Components

  Any safety critical components should be validated and certified through the appropriate industry standard, rule or best practice associated with the component, including assessment of their code safety.

- ✓ Warnings and Instructions

  Warnings and instructions should be relied upon only when other more reliable forms of intervention, such as elimination of a hazard or a guarding strategy, are not feasible. Warnings may be presented to consumers in many types of media (on-product text and graphics, paper-based hardcopies or any type of electronic media).

- ✓ Parental Controls

  Products to be used in homes should be expected to be accessed by children some of the time. Allowing caregivers to prevent use by children with passwords or other authentications, physical obstacles or other means should be considered.

- ✓ User Authentication and Confirmation

  Commands that requires an affirmative response from the user before executing may help prevent unintended activations of potentially hazardous events or conditions. In safety critical applications, where sensors indicate unsafe conditions, confirmations should be blocked until the conditions return to a safe status.

- ✓ Redundant Safeguarding

  Sensors or actuators that govern a potential safety device may contain back-up or secondary systems to prevent failures. Supervisory circuits can mitigate the effects of electrical failures. Where possible, physical safeguards for redundancy should be preferred to software safeguards.

- ✓ Information Security

  Always follow the best practices recommended by industry and government experts in information security from the outset of product design and throughout manufacture and deployment. (See Appendix B.)

- ✓ Consumer Information for Component Tracking

  Provide consumers with adequate information to determine the sources of device components so that threats and product updates can be traced during the lifespan of a product for use during recalls or product safety announcements.

- ✓ Consumer Information about Data Collection

  Ensure transparency in data collection, data sharing, and data use so that consumers can make informed decisions about their own data and any potential risks that may arise from the repurposing of that data. Ensure clear privacy policy statements.

✓ Consumer Information about Expected Lifespan

Provide lifespan expectancies of products and the anticipated duration of post-distribution support that will be provided by the manufacturer. Most importantly, provide an explicit statement of the potential hazards of using a product longer than its expected lifespan. Lifespan expectancies may not be known at the time of purchase, but can be provided to owners as an update when this information becomes known.

IV. Additional Safety Considerations for Special Product Types

Certain types of products may require additional considerations. This list is not comprehensive, but may provide a starting point for initial evaluations of a product.

✓ Products worn on or in the body (“wearables” or implants)

Address information security and privacy, acoustic hazards, the potential for and effects of thermal burns, chemical burns, toxic exposures, allergic reactions, ingestion hazards, galvanic skin responses, sweat, potential modifications to alter the fit and comfort of a device, environmental isolation of users’ senses and potential for distraction of users during safety critical activities. Power sources like coin cell batteries or lithium-ion batteries may require special instructions for the safest charging and discharging procedures for the batteries. Medical devices, or consumer devices with medical functions, should follow FDA guidance and applicable regulations (for more information see https://www.fda.gov/MedicalDevices/default.htm.

Address risks of defects, flaws, vulnerabilities, malfunctions, performance manipulation of the product, overheating, fire and compromises leading to potential criminalization/weaponization.

✓ Products used in nurseries (baby monitors, connected juvenile products)

Address information security and privacy, noise, strangulation on cords, light exposure, thermal hazards (heat and cold), and suffocation on plush items, positional asphyxia, small parts, and sharp edges.

Address risks of defects, flaws, vulnerabilities, malfunctions, performance manipulation of the product, overheating, fire and compromises leading to potential criminalization/weaponization.

✓ Products used in private spaces (like home security and monitoring devices, voice –activated speakers)

Address information security and privacy.

Address reliability over product lifespan (aging effects), power failures, obsolescence, loss of connectivity, corruption or disruption of functionality during updates.

Address risks of defects, flaws, vulnerabilities, malfunctions, performance manipulation of the product, overheating, fire and compromises leading to potential criminalization/weaponization.

- ✓ Products used in public spaces

Address risks of defects, flaws, vulnerabilities, malfunctions, performance manipulation of the product, overheating, fire and compromises leading to potential criminalization/weaponization.[1]

- ✓ Products used in vehicles

Address driver distraction.

Address extreme heat/cold, vibration, electromagnetic interference with vehicle functions and neighboring vehicles, interactions with crash protection devices such as airbags and seat belts, integration and unintended interactions with smart vehicle systems in the vehicle and in other vehicles sharing the road as well as local and national traffic systems.

Address risks of defects, flaws, vulnerabilities, malfunctions, performance manipulation of the product, overheating, fire and compromises leading to potential criminalization/weaponization.

- ✓ Products used in extreme environments

Anticipate the expected and foreseeable misuse environments and extreme conditions that a product will experience throughout the entire lifespan of the product.

Address risks of defects, flaws, vulnerabilities, malfunctions, performance manipulation of the product, overheating, fire and compromises leading to potential criminalization/weaponization.

- ✓ Products connected to “inherent hazards”

This category includes products that can release energy or toxins – “hazards in themselves,” such as stoves, ovens, furnaces, fireplaces, toasters, irons, lawnmowers, medicine dispensers, pipeline/tank valves, winches, gates, elevators, lifts, etc.

1. Products that are intended to activate or release hazards
    - o Address accidental activation (medicine dispensing device that is activated too often, giving patient too much medicine; pocket dial a

[1] For more information see https://copyright.gov/1201/2015/fedreg-publicinspectionFR.pdf p. 50-51 and https://www.copyright.gov/policy/1201/section-1201-full-report.pdf p. 75

storage tank valve releasing gas or turning on a heat source such as an oven). Consider authentication and confirmation protocols for all actuators and their control components.

  - Address intentional remote operation without direct supervision by the user (leaving a dishtowel on a stove, activating the stove on the way home from work, catching the towel on fire).

  - Address unintentional remote activation and automated activation.

  - Address risks of defects, flaws, vulnerabilities, malfunctions, performance manipulation of the product, overheating, fire and compromises leading to potential criminalization/weaponization.

2. Products that are not intended to activate inherent hazards but may be used by consumers in unintended ways (foreseeable, accidental or criminal) to control an inherent hazard

  - Address modularity, system building blocks that can be combined with hazardous products (example: a simple on/off switch attached to a power outlet for anything plugged into that outlet, then used with a power tool or a space heater that contains an inherent hazard).

  - Address unintentional activation with countermeasures commensurate to the possible hazards.

  - Address risks of defects, flaws, vulnerabilities, malfunctions, performance manipulation of the product, overheating, fire and compromises leading to potential criminalization/weaponization.

✓ Products that respond to hazards

This category includes products that respond during hazardous events (like fire sprinklers, airbags, CO alarms, insulin dispensers, pacemakers) to protect public health or treat a disease or illness, etc.

  - Address reliability over product lifespan (aging effects), power failures, obsolescence, loss of connectivity, corruption or disruption of functionality during updates.

  - Consider appropriate engineering redundancies, fail-safes, and supervisory circuits and/or other controls to limit critical failures.

  - Address false alarms, unintended activations leading to credibility questions (crying wolf).

    - Address risks of defects, flaws, vulnerabilities, malfunctions, performance manipulation of the product, overheating, fire and compromises leading to potential criminalization/weaponization.

- ✓ Products that isolate users from their surroundings

  This category includes products that cover or interfere with a user's senses (virtual or augmented-reality equipment, audio playback equipment)

    - Address expected use conditions/environments and foreseeable misuse conditions.
    - Consider warnings prior to or during activation of isolating features.
    - Address risks of defects, flaws, vulnerabilities, malfunctions, performance manipulation of the product, overheating, fire and compromises leading to potential criminalization/weaponization.

- ✓ Products that distract users or bystanders

    - Address expected use conditions/environments and foreseeable effects of distraction.

    - Consider warnings prior to or during activation of distracting features.

    - Address risks of defects, flaws, vulnerabilities, malfunctions, performance manipulation of the product, overheating, fire and compromises leading to potential criminalization/weaponization.

- ✓ Products that monitor people

  This category includes products that allow others to see, hear, locate, or track other people.

    - Address information security and privacy.

    - Address risks of defects, flaws, vulnerabilities, malfunctions, performance manipulation of the product, overheating, fire and compromises leading to potential criminalization/weaponization.

APPENDIX A

The documents listed below contain hypertext links or pointers to information created and maintained by other public and private organizations. These links and pointers are provided for the users' convenience. Commissioner Kaye does not control or guarantee the accuracy, relevance, timeliness, or completeness of this outside information. Further, the inclusion of links or pointers to particular items is neither intended to reflect their importance nor endorse any views expressed, or products or services offered, on these outside sites, or the organizations sponsoring the sites

1. Cybersecurity resources:
https://doi.org/10.6028/NIST.IR.8228-draft
https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot
https://www.nist.gov/publications/framework-cyber-physical-systems-volume-1-overview
https://www.gov.uk/government/publications/secure-by-design
https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security
https://www.microsoft.com/en-us/sdl
https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices
https://www.nccgroup.trust/globalassets/our-research/uk/whitepapers/2014-04-09_-_security_of_things_-_an_implementers_guide_to_cyber_security_for_internet_of_things_devices_and_beyond-2.pdf
https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf
https://www.bsimm.com/framework.html
https://github.com/OWASP/samm/raw/master/v1.5/Final/SAMM_Core_V1-5_FINAL.pdf
https://www.owasp.org/index.php/IoT_Security_Guidance
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
https://www.owasp.org/index.php/IoT_Testing_Guides
https://www.owasp.org/index.php/Security_by_Design_Principles
https://aws.amazon.com/compliance/security-by-design/
https://standardscatalog.ul.com/standards/en/standard_2900-1
https://www.iec.ch/whitepaper/iotplatform/
https://www.iso.org/standard/65695.html?browse=tc (ISO/IEC 30141:2018 – Internet of Things (IoT) – Reference Architecture

2. Internet of Things White Papers:

a. Cassidy, Tim & Xu, Eric (2018) “Consumer Product Safety in an IoT World: A white paper”, Society of Product Safety Professionals, https://www.productsafetyprofessionals.org/s/Physical-Safety-in-an-IoT-World-4.pdf.
b. OECD (2018), "Consumer product safety in the Internet of Things", OECD Digital Economy Papers, No. 267, OECD Publishing, Paris, https://doi.org/10.1787/7c45fa66-en.
c. ANEC/BEUC/CI/ICRT (2017) “Principles and Recommendations 'Securing consumer trust in the Internet of Things”, http://www.anec.eu/images/Publications/position-papers/Digital/ANEC-DIGITAL-2017-G-054.pdf.
d. UL (2016) “An Introduction to the Internet of Things”, Underwriters Laboratories, https://library.ul.com/wp-content/uploads/sites/40/2016/02/Internet-of-Things-white-paper_final.pdf.pdf.

3. User-centered design best practices are available:

a. The Application of Human Factors to Consumer Products

https://www.cpsc.gov/s3fs-public/HF-Standard-Practice-Draft-12Feb2018.pdf?CGk4Zs9GabjCnZ5RXQuSlr2toQ1aLPhJ

b. The Application of Human Factors to Consumer Products: ANNOTATED BIBLIOGRAPHY

https://www.cpsc.gov/s3fs-public/Annotated_Bibliography.pdf?FHaLb3lSrsc1QGRThcpH8998uWUyx4kv

4. Effective **warnings and instructions** resources can be found here:

Singer, J. P., Balliro, G.M., & Lerner, N. D. (2003) “Manufacturer’s Guide to Developing Consumer Product Instructions”, T. P. Smith (Editor), U.S. Consumer Product Safety Commission, Contract No.: CPSC-S-02-1215. https://www.cpsc.gov/s3fs-public/pdfs/guide.pdf.

APPENDIX B

The documents listed below contain hypertext links or pointers to information created and maintained by other public and private organizations. These links and pointers are provided for the users' convenience. Commissioner Kaye does not control or guarantee the accuracy, relevance, timeliness, or completeness of this outside information. Further, the inclusion of links or pointers to particular items is neither intended to reflect their importance nor endorse any views expressed, or products or services offered, on these outside sites, or the organizations sponsoring the sites

1. The Federal Trade Commission (FTC) has described the following best practices **for data security**:

1. Start with security.
2. Control access to data sensibly.
3. Require secure passwords and authentication.
4. Store sensitive personal information securely and protect it during transmission.
5. Segment your network and monitor who's trying to get in and out.
6. Secure remote access to your network.
7. Apply sound security practices when developing new products.
8. Make sure your service providers implement reasonable security measures.
9. Put procedures in place to keep your security current and address vulnerabilities that may arise.
10. Secure paper, physical media, and devices.

From FED. TRADE COMMISSION, START WITH SECURITY: A GUIDE FOR BUSINESS (June 2015), https://www.bulkorder.ftc.gov/system/files/publications/pdf0205-startwithsecurity.pdf.

2. The FTC has also described best practices **specific to connected devices**:

- Start with the fundamentals.
  - Encourage a culture of security.
  - Implement "security by design."
  - Implement a defense-in-depth approach.
  - Take a risk-based approach.
  - Carefully consider the risks.
  - Avoid default passwords.
- Take advantage of what experts have already learned about security.
  - Use standard encryption techniques.
  - Add "salt" – random data – to hashed data.

Consider using rate limiting.

Design your product with authentication in mind.

Protect the interfaces between your product and other devices or services.

Consider how to limit permissions.

Take advantage of readily available security tools.

Test the security measures before launching your product.

Select the secure choice as your default setting.

Use your initial communications with customers to educate them about the safest use of your product.

Establish an effective approach for updating your security procedures.

Keep your ear to the ground.

Sign up for updates from trusted security sources.

Check free databases of vulnerabilities identified by vendors.

Maintain a channel where security researchers or consumers can reach you.

Consider bug bounty programs to reward people who identify vulnerabilities.

Innovate how you communicate.

Use a set-up wizard to implement security features.

Build in a dashboard or profile management portal for security settings.

Let consumers set up "out of band" communication channels.

Use icons, lights, or other methods to signal when an update is available.

Let prospective customers know what you're doing to secure customer information.

From FED. TRADE COMMISSION, CAREFUL CONNECTIONS: BUILDING SECURITY IN THE INTERNET OF THINGS (Jan. 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf.

3. A non-profit organization, the **Online Trust Alliance and the Internet Society** (ISOC), provide a framework of principles for securing IoT devices that was developed through a consensus driven, multi-stakeholder process. Their best practices include security principles; user access and credentials; privacy, disclosures and transparency; and notifications and related best practices available at:
https://www.otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

[January 2019]